PRIVACY LEGISLATION AND ITS IMPLICATION TOWARD THE COMPUTER INDUSTRY

Carol Jean Janssens

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

Privacy Legislation and its Implication
Toward the Computer Industry

by

Carol Jean Janssens

June 1977

Thesis Advisor: N. F. Schneidewind

Approved for public release; distribution unlimited

SECURITY CLASSIFICATION OF THIS PAGE (When Date Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. / 3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle): Privacy Legislation and its Implication Toward the Computer Industry	5. TYPE OF REPORT & PERIOD COVERED: Master's Thesis: June 1977
	6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): Carol Jean Janssens	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Naval Postgraduate School, Monterey, California 93940	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS: Naval Postgraduate School, Monterey, California 93940	12. REPORT DATE: June 1977
	13. NUMBER OF PAGES: 51
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): Naval Postgraduate School, Monterey, California 93940	15. SECURITY CLASS. (of this report): Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Privacy
Security

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis researched the effect major legislation in the area of individual privacy has on the computer industry. Definitions and current legislation are discussed. Specifically, the influence of privacy legislation in the following areas

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601 |

SECURITY CLASSIFICATION OF THIS PAGE (When Date Entered)

was considered: Management, Data: Accuracy and Flow, Hardware, Software and Cost. Certain recommendations for implementation of legislative requirements and problems created by existing regulations are discussed.

Approved for public release; distribution unlimited

PRIVACY LEGISLATION AND ITS IMPLICATION TOWARD THE COMPUTER INDUSTRY

by

Carol Jean Janssens
Lieutenant, United States Navy
B.S., Northwestern State College, 1970

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL

June 1977

ABSTRACT

This thesis researched the effect major legislation in the area of individual privacy has on the computer industry. Definitions and current legislation are discussed. Specifically, the influence of privacy legislation in the following areas was considered: Management, Data: Accuracy and Flow, Hardware, Software and Cost. Certain recommendations for implementation of legislative requirements and problems created by existing regulations are discussed.

TABLE OF CONTENTS

I. INTRODUCTION

Previous to the enactment of the "Privacy Act of 1974", the main thrust of computer literature was toward the depth to which the laws of this country should regulate personal information processed by computers and the extent to which individual privacy needed to be safeguarded. It is not unusual to obtain a copy of one of the many "horror stories" associated with computers or to see a comic of an individual's life being threatened by the invalid, inaccurate information in a computer. What was not emphasized, however, is that the machine itself is not the villain: the processing of the contents of that machine by human beings is the crux of the issue.

The purpose of this thesis is to discuss some of the more recent issues on individual privacy and security related to the Computer Industry today and determine exactly what computer professionals should focus on to implement today's legislation.

A basic definition of privacy and security will be discussed along with the "Privacy Act of 1974" and its implications toward computer operations. The influence of this legislation in the following areas will be considered:

1. Management
2. Data : Accuracy and Flow
3. Hardware Considerations
4. Software Considerations
5. Cost

A. DEFINITIONS

Privacy is "the right of individuals, groups or organizations to control the collection, use, or dissemination of personal identifiable information." [24] In another context, the meaning of privacy is the right to be left alone. The former definition, most accepted in the industry today, is assuredly less restrictive in nature since it justifies record-keeping systems and disregards the question raised by the latter of the right to gather any personal information whatsoever.

Security is "the realization of protection for hardware, software, and data." [24] In this sense, privacy therefore implies protecting the individual whereas security protects the organization. In order to maintain privacy, enforcement of security is necessary. It is understood that one area cannot be considered without overlapping into the other.

To establish clarity, the following definitions are quoted from section 552(a) of the "Privacy Act of 1974". [54]

The term 'agency' includes Federal agencies and those government contractors who maintain a system of records to accomplish a function of a Federal agency. Subdivisions of an agency may be defined as agencies. It is determined by the higher unit as to which of its components will be subject to the Freedom of Information Act rather than the Privacy Act. This practice of allowing flexible internal compliance is intended to further the purpose of the acts, not to defeat them. [49]

"The term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." [54]

The intention of this definition is to "distinguish between the rights which are given to the citizen as an individual under this Act and the rights of proprietorships, businesses, and corporations which are not intended to be covered by this Act. This distinction was to insure that the bill leaves untouched the Federal Government's information activities for such purposes as economic regulations. This definition was also included to exempt from the coverage of the bill intelligence files and data banks devoted solely to foreign nationals or maintained by the State Department, the Central Intelligence Agency and other agencies for the purpose of dealing with nonresident aliens and people in other countries." (Senate Report 93-1183, p. 79).

"The term 'maintain' includes maintain, collect, use, or disseminate." [54] Within the Privacy Act, two connotations of "maintain" are used: first, to denote the record keeping actions which apply to the act; and second, control (not necessarily physical custody) over, and thus responsibility and accountability for record systems.

"The term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." [54]

"A "record" :

- means any item of information about an individual that includes an individual identifier;
- includes any grouping of such items of information (it should not be confused with the use of the term record in the conventional sense or as used in the automatic data processing (ADP) community) ;
- does not distinguish between data and information; both are within the scope of the definition; and
- includes individual identifiers in any form including, but not limited to, finger prints, voice prints and photographs." [49]

As is stated later, understanding this definition is imperative in determining exactly which requirements of this legislation apply to each computer system of records. Record as used in the Privacy Act extends beyond the conventional computer science context. It can include one descriptor about an individual or many descriptors. Therefore what is considered a data field or group of fields in a computer record could be established as a record in the legal sense. This means that a computer record could consist of many legal records.

"The term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. [54] The key phrase in this definition is 'retrieved by'. Those records which are not obtainable by use of a 'personal identifier' are excluded from the act even though the possibility of using the 'identifying particular' as a key field in record retrieval exists. According to the Office of Management and Budget (OMB) Guidelines, 'agencies' should consider two

factors in determining which systems are covered: "....its ability to comply with the requirements of the Act and facilitate the exercise of the rights of individuals; and ....the cost and convenience to the agency, but only to the extent consistent with the first consideration." [49] Also, section 552k(4) lists specific exceptions to those systems of records covered by the Act.

"The term 'statistical record' means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13." [54]

"A "statistical record", for purposes of this Act, is a record in a system of records that is not used by anyone in making any determination about an individual. This means that, for a record to qualify as a "statistical record", it must be held in a system which is separated from systems (some perhaps containing the same information) which contain records that are used in any manner in making decisions about the rights, benefits, or entitlements of an identifiable individual, The term "identifiable individual" is used to distinguish determinations about specific individuals from determinations about aggregates of individuals as, for example, census data are used to apportion funds on the basis of population.

By this definition, it appears that some so-called "research records" which are only used for analytic purposes qualify as "statistical records" under the Act if they are not used in making determinations. A "determination" is defined as "any decision affecting the individual which is in whole or in part based on information contained in the record and which is made by any person or any agency." (House Report 93-1416, p.15.)

Most of the records of the Bureau of the Census are considered to be "statistical records" even though, pursuant to section 8 of title 13, United States Code, the Census Bureau is authorized to "furnish transcripts of census records for genealogical and other proper purposes and to make special statistical surveys from census data for a fee upon request." (House report 93-1416, p. 12)

In applying this definition, it might be helpful to distinguish three types of collections or groupings of information about individuals: (1) statistical compilations which, because they cannot be identified with individuals, are not subject to the Act at all; (2) "records" maintained solely for the purpose of compiling statistics - which are the types of records covered by section 552(a)(6) of the Privacy Act; and (3) "records" on individuals which are used both to compile statistics and also for other purposes, e.g. a criminal history record used both to compile individual statistics and to assist a judge in making a sentencing decision about the individual to whom the record pertains, which is not a "statistical record." [49]

"The term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." [54]

B. LEGISLATION

In legislating, the right of privacy must be balanced against equally valid public interests in freedom of information, national defense, foreign policy and law enforcement.

On the international level, there have been three approaches to the regulation of privacy:

1. Administrative self-regulation which was employed by the British.
2. Omnibus licensing and regulation, the approach of Sweden and Germany.
3. An area-by-area provision of court enforceable citizen rights which is the American viewpoint.

The British "Data Surveillance Bill of 1969" establishes a Registrar to keep a register of all data banks, public and private. This register contains details of the data kept by the data bank, the person responsible for the dat bank, the purpose for which data may be used, and by whom. The register is subject to both public and private inspections. Under this bill, each person shall receive a printout of the data stored about himself including the purpose for which it is used when the data bank is established.

Afterward, for a fee the individual may obtain a printout of the data, their purposes and a listing of all the recipients of such data. If an individual desires to remove inaccurate, unfair or out of date information, he may apply for an order to remove such data and all recipients are notified. The law further states that each operator of a data bank is liable for damages when he permits inaccurate data to be supplied which can be harmful to a person. Punishable offenses include failure to accurately register a data bank, use of the data for nonregistered purposes, allowing access to persons other than those entered on the register, and aiding and abeting the wrongful use of the data.

Various West German States have passed data protection acts that establish certain measures of control over government files. Sweden, the first country to pass a law on privacy, established a federal Data Inspection Board. This organization requires the licensing of all commercial, computer-operated record-keeping systems in accordance with established government standards including conditions for their operation. The board additionally provides advice on the conduct of government data banks.

France has studied the problem, but has taken no definitive action. The Department of Communication and Justice in Canada has produced substantial studies and recommendations on the issue of privacy, however, no legislation has been passed at this time.

It is of special importance that Canada and the United States be strengthened in the area of privacy regulation because of the enormous number of privately owned American companies headquartered in Canada and the United States.

Questions regarding the legal regulation and restrictions on the private records of Canadian citizens which are owned by American companies are still unanswered.

The concern over invasion of privacy has received special attention in the United States as a result of numerous developments, among which are the GSA proposal for a comprehensive computer network which could store personal information on file in several different Federal agencies, and increasing use of the social security number as a standard universal identifier.

Since policy conflicts arise, as in all government legislation, two approaches are taken to resolve these

differences. The agency-by-agency resolution which imposes upon each agency "....the responsibility for regulating dissemination of personal data persuant to legislative guidelines - including the duty to obtain first the written consent of the subject." [32] This approach fixes responsibilities, however, some agencies may have to expand their own information collecting activities to obtain directly from the subject what previously was obtained indirectly from other agencies. The second approach classifies and regulates programs and types of data systems. "This approach relieves the burden on some agencies, but would not distinguish the portions of such records which could usefully and properly be disclosed". [32] A combination of both approaches has been implicit in most bills introduced in Congress, but the need for a study of the proper balance of the values in conflict still arises. One reason for this discord is that presently there is no legal definition for privacy. It has been established, however, that each individual's idea of privacy differs with age, experience and environment.

The "Privacy Act of 1974" (P.L. 93-579) amends Chapter 5 of Title 5 of the United States Code (section 552a). It applies to U.S. Federal Government Agencies and private contractors who are performing a record-keeping service for a Federal agency and is based on the 1973 report by the Committee on Personal Data Systems of the Department of Health, Education and Welfare entitled "Records, Computers and the Rights of Citizens". [55] This landmark in computer history created a set of standards for the collection, maintenance, use and dissemination of personal information in both manual and automated systems. The initial report contained a set of 'fair information practices'.

The purpose of the Code of Fair Information Practices was to define the desired behavior of a data bank, the

desired relation between the data subject and the data bank, and to establish certain rights for each citizen. Each of the five basic principles was incorporated into the Privacy Act:

1. There must be no personal data record-keeping system whose very existence is secret.

2. There must be a way for an individual to find out what information about him is in a record and how it is used.

3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data. [55]

These principles as incorporated in the Privacy Act (section 552(b)) include the permitting of exceptions to the Act when determined by specific statutory authority.

1. Provisions are provided which require the publication of an annual notice in the Federal Register and public notice of changes to existing systems of records as well as new systems.

2. Any individual is permitted to view and receive a copy of any record containing personal information about him

in those systems covered by the Act exclusive of exempt disclosures. He may also see an accounting of his record to determine how the information in it has been used.

3. Unless prior written consent has been obtained from an individual, all Federal agencies are prohibited from disclosing information unless its use is consistent with the original intent of the collection of such information.

4. The Privacy Act specifies procedures which must be implemented by the agencies to allow an individual the possibility of amending or changing his record. Additionally, it requires that said agencies must review initial refusals to amend such records and state the reason for this action.

5. All subject records used by an agency which maintains the system of records shall insure their accuracy, relevance, timeliness and completeness "as is reasonably necessary to assure fairness to the individual." [54] These agencies are to implement administrative, technical and physical safeguards "to insure security and confidentiality of records." [10]

Additionally, the Privacy Act clearly states that responsibility for effective personal information systems and integrity and accuracy of the data which comprise them, rests with those individuals who manage and employ such systems. If this law is not implemented, civil penalties will be awarded.

II. EFFECT ON COMPUTER SYSTEMS

In section 552e of the Privacy Act, certain requirements are listed for each agency to fulfill. To implement these conditions, the Office of Management and Budget Privacy Act Guidelines of July 1, 1975 have been created to further explain the measures to be enacted. Since it is the responsibility of the personnel who maintain the record systems covered by the Privacy Act to insure the accuracy and integrity of personal information, certain procedures should be established and fulfilled to comply with this legislation. Although, it is beyond the scope of this discussion to list precisely what must be accomplished in each computer installation, those measures applicable to all situations will be mentioned. By studying the installation and establishing the objectives and goals to be attained in specific circumstances, an efficient review and plan of action can be developed with the least amount of effort.

A. MANAGEMENT CONSIDERATIONS

The first consideration is to decide which systems of records are covered under the Privacy Act. This may seem a simple task: however, due to the vague and complex definition in the law, serious thought and study should be spent on this decision. This leads to the necessity of a manager knowing the current legislation. (The Privacy Act and OMB Guidelines are in the forefront today. Among other pertinent literature is the Freedom of Information Act and H.R.1984). Realizing that not all managers have the time to

read the legislation, nor the legal expertise necessary to understand all the implications or details, the need for education arises. An alternative approach would be to appoint individuals knowledgeable in both fields, law and computer science, to study the situation and present a summary (in layman's terms) available to all computer installations. This would not only save much time and avoid unnecessary complications, but would be an excellent mode of educating a vast number of computer professionals in a short time. It is inevitable that private industry will be affected within the next three years and the need for rapid understanding is mandatory. Various states have legislation already in effect.

There are measures to protect computer professionals which can be accomplihed before more legislation goes into effect. The Association for Computing Machinery has suggested rules of conduct for personnel in the computer industry. These guidelines cover three categories of professional conduct: relations with the public, relations with employer and clients, and relations with other prcfessionals.

To insure a high quality of personnel, it is desirable to establish similiar standards throughout the profession. Other approaches, previously mentioned in literature, have been licensing or bonding of personnel and certification. By insuring the competence and integrity of personnel, the installation thus increases protection against illegal activities, intentional or not, and decreases the threat of internal subversion. These standards must continue to demand high quality work. This means accuracy of data. More will be said of this in later sections. In addition to the personnel, assurance of adequate physical protection should be established. The National Bureau of Standards and the Association of Computing Machinery have published

security checklists as guides in determining proper security at each installation. [24,46] These are excellent starting points in planning the protection of an organization regardless of the age or style of the computer equipment. Questions applicable to all phases of computer technology will be found in these references.

Presently, there is some level of security at all installations. Controlled personnel access to the computer is an important factor in maintaining secure operations. There are various ways to attain restricted entrance. The point here is to consider who has the authority to obtain admission to the facility and how difficult it is for an unauthorized individual to achieve access. The next step is to determine which method to use and to what degree, if any, restricted access is necessary. The computer environment should not be overlooked in deciding how to implement protection measures. The location of the facility and the building in which it is housed, if poorly guarded and constructed, may lead to infiltration and destruction of personal information or other valuable files. Thus computer personnel could be accused of negligence and appropriate penalties would be awarded.

Once the overall physical environment has been analysed and appropriate decisions made as to what action, if any, is required, the computer equipment and software should be evaluated for compliance. After a final review of the equipment and support facilities, the final step is to provide for future analysis, otherwise known as periodic auditing. There are various methods for accomplishing a reevaluation of existing systems. One of the most effective being management by exception. This does not preclude the possibility of other less important factors influencing the quality of an efficient system, but rather aids in

establishing which attributes most significantly hamper computer operations and implementation of objectives.

Before concluding this portion of the discussion, a remark on costs should be included. Those elements which must be weighed in management of computer facilities all contribute to some degree to the cost of compliance. The basic question to be resolved is which action should be taken at a reasonable expense. If every computer installation takes a passive role toward the legal implications and responsibilities set forth by government, have the efforts of individuals to maintain their right to privacy and their right to have accurate facts pertaining to their lives contained in these machines been for nought? Does this attitude reflect the typical manager's position.....is this an enhancement or hindrance to the computer profession? Should every manager wait until the other organization is penalized or should he use the prudent man approach? It is suggested that each computer facility review its operations and procedures, then a decision as to what degree of compliance is necessary would be made to the benefit of the entire community.

B. DATA : ACCURACY AND FLOW

This section will discuss those factors which influence how data is collected and what factors affect the quality of exactness achieved in information retrieval. The various methods employed in data collection have a commonality of factors which influence the degree of accuracy attained in initial accummulation. The nature of the data may cause unavoidable error. For example, if the specific numeric, alphabetic or special characters are written in an undecipherable penmanship it is left to the descretion of

the individual who enters that data into the computer system as to whether it is correct or not. This is not to say mistaken data is intentionally created, but obviously the need for validation arises. Which validation procedure is implemented is the decision of those personnel responsible for data accuracy. Analysis of input data should include whether or not a particular item is still necessary for the purpose for which it was intended. If the data is no longer required, it should be deleted from the input procedures. Retention of data for longer than needed could also cause harm to individuals. There is no standard time for determining when this information is obsolete as this depends on the status of its function, i.e. if this purpose was satisfied, or the age of the information causes it to be unreliable, or if its only value is historical. Other elements involved in error control and collection include the authority for assembling the data, who does the actual collection and why. Not to be missed is the source of the data. If the data collected is not correct initially, error checking at the computer center level may not be effective. The legal implication, of course, is: Who is responsible, the individual who inserted false data or those who maintain it?

The legislative view is to assume a relationship of trustworthiness between the data subject and the receiver of the information. If the individual for whatever motive, enters false data into the system, how does the computer industry protect itself against lawsuits for invalid data? Idealistically, this situation would never arise. Realistically, protection of both parties should be established.

The form which contains the data should be examined for clarity and readability. A poorly designed document can lead to errors by the most well-intentioned procedure. If

that data is not inscribed directly into the system, such as from a terminal, are the initial forms (source documents) which contain that information carelessly discarded or is some procedure implemented to insure those documents do not reach unauthorized personnel?

This leads to protection of the data once it has been entered into the system. Determinations as to the possibility of maintaining dedicated systems for personal information files could lead to excessive costs and management adversity. This approach could be justified by the stringent requirements of security and the threat to individual privacy. The costs of maintaining a separate system and losing the benefits of a shared data base are factors which should be weighed in this decision. Integrating data into a data base may not be the problem if the elements (identifying particulars) have no purpose in being in that specific data base at all. The sensitivity of the personal data may vary thereby lending itself to levels of classification. Since the legislation may cause problems, existing record structure needs to be examined for legal records to establish what data fields may have to be changed to conform to the legal requirements. The mixing of the different sensitivity levels of data and sensitivity transience have created the need for reevaluation at the data field level. Presently, the technological approaches to store mixed levels of data either use an increased amount of storage or an immense amount of time. The existing technology for file structures does not have a simplified solution to this situation. The idea of simple aggregation of data such as statistical information has been suggested to alleviate this problem. The intent is that having a large number of records, even with certain sensitive elements contained in the record, will be sufficient to eliminate the threat of harm to an individual. One method is to input individual items, compute aggregate (averages,

etc), then destroy inputs. This is adequate if the organization only needs aggregates. Obviously, if the sensitive information is still in the data base after aggregation, no protection has been afforded. This 'safety in numbers' attitude could be a simple method to employ, but does not insure that an unauthorized individual is prevented from obtaining the information in the files. Even if the sensitive information was given some serial number and cross referenced on another higher level file, this does not preclude the possibility of unauthorized access to the personal information.

Software utilities may alter or delete personal information. This action substantiates the need for establishing a check of existing programs for compliance with the current legislation. If unintentional modifications to legal records occur, further errors are created. The programs required to process the information should not increase fallacy in the process and decrease data integrity. By refusing to evaluate current software, the threat of individual harm persists. Checks to include privacy compliance in new programs should be added to current standards. This insures continued protection of individual rights and data integrity. Operating systems have been studied and designed around security, but existing systems are not totally immune to illegal penetration. To consistently patch holes and use the retrofit approach certainly does not insure unauthorized access and may create new paths of entry.

It is a fact in our industry that a software approach to insuring security of files is only as effective as the hardware in which it is stored. Faulty machinery which loses bits of data creates errors. Proper preventative maintenance aids in maintaining a secure system. The eavesdropping or "bugging" of electronic devices is

presently being researched. New methods of eliminating electronic fallout are being tryed and possible solutions exist in the near future. Currently, however, the problem still exists. What are the legal implications if personal information is obtained in this manner? How is one to provide for protection of personal information if current technology has nct advanced to the degree of furnishing a solution? Are the responsibilities of the computer industry to perhaps revert to simpler methods of processing information by eliminating third generation equipment and networks? This question, although harsh, is to point out the need for legislative personnel and computer personnel to work together in solving data processing problems. To formulate realistic legislation toward computer processing entails careful deliberation on all phases of the industry coupled with the rights of the individual at a reasonable expense to all.

Once the information has been generated, procedures for insuring proper safeguards for output should be maintained. Legal restrictions and verification of reports, tapes, cards, etc, for 'routine use' and 'the purpose for which originally intended' pose a problem of revising production procedures. The same possibilities of unintentional disclosure exist as with original input. Certain precautions may include changing the output class so that computer operators may administratively provide a more secure environment for the output. For example, running those printouts only at certain times and allowing only the individual who submitted the job to receive the output or re-locating a printer to a more restricted area where only authorized personnel would see the information. If carelessly discarded output is not destroyed, and unauthorized uses result, legally it is the responsibility of the computer facility and civil action may follow.

C. HARDWARE CONSIDERATIONS

"Physical security measures are the first line of defense against the risks which stem from the uncertainties in the environment as well as from the unpredictability of human behavior." [46] Computer architecture is not designed to fully eliminate the ability to obtain access to data through unauthorized methods. Some devices for insuring protection include memory protection schemes such as relocation and bounds registers, segmentation, paging and memory keys which allow limited access i.e. read-only. Error-detecting circuits and codes check almost all hardware errors in the computer. The problem of insuring privacy of data from a hardware standpoint includes those older machines which do not have current technological features incorporated into their structure and the retrofit solution has not been successful in resolving illegal penetration. Regarding networks, the greatest potential of a break in security lies in the telecommunications line. Electronic emanations are the greatest threat. As stated previously, solutions to this problem are being studied and a workable result is expected soon. [47]

1. Operating System

The third-generation computer with operating systems or master control programs have, generally, two modes of operation: supervisor (system) and problem (user). The supervisor mode enables one to execute priviledged instructions. These instructions include changing the state of the computer, starting input/output processors, changing protection rights of parts of the computer and altering the interrupt status of the machine. Obviously, one who has access to the supervisor mode for a specific computer has

access to any and all data associated with that computer. Previous cases of a user, intentionally or not, entering the supervisor state for harmful reasons have been recorded.

One solution to avoiding this situation has been the 'patchwork' approach. When one "hole" was patched, another was created thereby initiating a more complex path to achieving the goal of illegally retrieving data. The procedures to insure that the supervisor mode is not obtained through illegal methods have so far not proven totally successful.

The storage protection mechanism in the operating system is a major factor in safeguarding personal data. Not only does it affect computer performance, but if not properly implemented and controlled, sensitive data could become available to an unauthorized user. "Common protection mechanisms are checks on logical addresses or on physical addresses. The logical address check consists of a segment base containing the actual address and the segment length. The physical address protection employs separate key-to-lock mechanisms." [24] The proper utilization of this mechanism coupled with limited read-only or write-only access to the programs and data within the computer decrease a possibility of alteration and access to personal data and increase compliance with present legislation. Limiting access to the master control program or operating system is another obvious safeguard to be employed.

2. Peripheral Devices

Consideration of direct access storage devices and tape drives includes the methods of erasing erroneous or out-of-date data contained on the medium. Therefore to insure security, writing over the entry could be

accomplished through hardware control while disconnected from the data channel. This method is preferred over the use of the operating system for this purpose since the latter may involve too many system services and extreme overhead.

Tape drives can best be protected through administrative procedures. The tape labeling process is easily bypassed and in some cases access to the data tape is obtained by merely requesting the tape be mounted. One proposed solution is to color code specific devices which contain personal information to easily determine the legal requirement for special protection. With regard to input/output devices, current designs are not adequately secure. Teleprocessing equipment provides the greatest threat of harm. In terminal systems, the need to identify the operator and terminal is real and valid. The solutions here vary from password to keyword voice spectro-analysis. In some cases sign-ons are accomplished through hardware control.

For unit record devices, limited access to the media and data through administrative measures is one solution. Error checking codes, i.e., parity and cyclic checking must be required for data protection; and logic circuit redundance is necessary in the core critical hardware circuitry.

D. SOFTWARE CONSIDERATIONS

Certain administrative procedures for software have been mentioned. It is the purpose of this section to discuss the technological aspects of programming with regard to privacy legislation.

The solutions mentioned in literature for software security have been costly and not necessarily realistic for the computer installation. For example, placing an indicator in each "legal record" has been suggested. This however requires space which may not be available and would require lengthening a computer record which may already be using all its allocated space. In older computer systems, storage techniques and programming are not as versatile as in newer systems and this implies obtaining a new computer system. Certainly this is not an easy task or decision.

There are various types of attacks involving software which have been categorized by the Air Force Panel on Technology and Planning. [3]

"In the case of implied sharing,the supervisor shares some of its work space with the problem programs. Therefore, the problem program is free to access such resources as the catalog, and buffers in which proprietary information is kept. For example, the supervisor reads the security profile (the list of system data sets and user passwords) into the user's area to authenticate the user that is requesting access to a particular data set (date file). However, because the information remaining in the shared area (the user's area) and has not been overwritten, the current user now has access to other users' passwords." [24]

Obviously, the solution is to eliminate both supervisor and problem mode using the same work space. This means redesigning the operating system. If the system includes checks for location and use of the supervisor and insures the space has been overwritten before assigning it to a problem program then this threat is eliminated. This of course delays use of system resources. The implication is

certainly not to be taken lightly---- there is no thoroughly secure system.

"In the case of scavenging, the word space is not shared by the user's program, but neither is it cleared after being used by the supervisor. Therefore, if the user has access to it, he could gain access to sensitive information like passwords and authorization levels. Another type of scavenging exists in the area of data management. On a direct access device, the system can allocate space for a file and then fill that file with sensitive data. When that file is deleted, its space may not be cleared by the system. Therefore, when another user program gains control, the system could allocate that same space to the user so it is possible for him to read it and gain access to sensitive information that was left there previously. Temporary files used in the course of a job that contained sensitive data could also be candidates for scavenging." [24]

To clear the workspace before it is used by the next job would eliminate this type of attack. Technologically, this problem has been solved and should not be a factor in larger systems. In smaller, less sophisticated computer systems, the flexibility of the operating system is limited and stricter administrative controls and procedures are used.

"Incomplete parameter checking is a major weakness of contemporary operating systems that occurs at the interfaces between the system and the users' programs. Users call operating system functions in a manner similar to subroutine calls, using many parameters. By supplying addresses outside the space allocated to that user's program, three dangerous results are possible:

1. The supervisor may obtain unauthorized data for that user.

2. A set of conditions can be generated to cause a system crash.

3. Control may be returned to the user in supervisor state." [24]

To assure control of the supervisor state is not gained through this means requires redesign of the storage protection mechanisms as well as limited access to those addresses wherein the supervisor resides.

"The asychronous interrupt method exploits a combination of poor system design and the handling of asynchronous interrupts. For example, suppose a remote terminal user is permitted two unsuccessful sign-ons before being terminated. When the system is designed to handle an interrupt before updating the counter used to limit this, unpredictable results can occur.

The trojan horse class of attack is used in an attempt to achieve the breakdown in security by introducing into the operating system programs with security holes. When a hole is activated, the "trojan horse" routine can be used to open any user files and gain access to classified data. For example, a software performance monitor, while evaluating a program, can gather sensitive data associated with that program.

The clandestine code change is a class of attack that is closely related to the trojan horse attack. In this case, system programmers could insert code into the system that would form trapdoors. Indeed it is almost routine for systems programmers to add such trapdoor code to current operating systems for legitimate systems programming purposes such as quick maintenance. At certain times and based on certain combinations these trapdoors may be

activated by a user from his program. This capability also exists for the persons who initially design the system, or for manufacturers who supply fixes to the system.

The asynchronous attack has often been referred to as the time of check and time of use problem. When a user's program parameters were originally checked by the supervisor they were proper. But after the check and before their use, the user changed them so as to circumvent some protection feature of the system. This attack is possible because third-generation computers are able to process input/output and relinquish control back to the user for concurrent processing." [24]

These threats involve a redesign of the operating system and stricter security measures in software development. Controlling user access to the supervisor mode is re-emphasized. The creation of a security matrix for purposes of deciding who has authorized access to which resources is mandatory. The solutions to those threats as yet unconquered rely on the technological community to provide the answer.

Legally, the question still remains: if it is technologically possible to gain access to personal information and the state of the art has not conquered the method of attack, who is liable? If the computer installation has implemented all possible procedures to avoid unauthorized access, are they still subject to legislative penalties? The possibility of designing a totally secure software operating system into existing hardware is not realistic and would be extremely costly. Therefore more reliable program design, acceptance testing and standards is an alternative approach.

Possible safeguards to be employed include: proper decision making criteria (for example including all appropriate factors and changing them as circumstances warrant), avoiding logic errors caused by an invalid translation of requirements between user and programmer, including a complete edit check for determining complete input data (this includes for instance a check for blank data fields leading to incomplete information), establishing standards and criteria for programming documentation.

In a study conducted by the Government Accounting Office (GAO), the following software problems were researched. They are quoted as possible areas of improvement for more effective control in implementing privacy legislation.

1. Adequate communication between the parties to software design.

2. Incorrect perceptions of the nature of actual transactions to be processed.

3. Inadequate documentation preventing adequate reviews of software.

4. Time constraints hampering the effectiveness of the design process.

5. Absence of written criteria or guidelines for designers to follow.

6. Detail and complexity involved in designing, coding, and reviewing software

7. Reliance on the expertise and experience of people doing the work.

8. Undetected changes in circumstances making the application obsolete.

9. State of the art of program testing which prevents testing all possible conditions. [22]

Certain solutions have been proposed to assist in the elimination of these sources of error. It is noted that with today's technology, completely error-free software cannot be designed, however the probability of inaccurate documentation can be reduced through implementation of applicable procedures.

"-Documentation should be prepared that highlights (1) key portions of the automated decisionmaking criteria, (2) data elements that are critical to the decisionmaking, and (3) the edit checks placed (or justifications for omitting them) in the software. A formalized synopsis of these items should be prepared for review and approval by top management.

-Qualified auditors or others who are independent of designers and users should review the designed application before it is placed into operation. Others could include a design team independent of the original designer and user. They would be responsible for evaluating the (1) adequacy of the decisionmaking criteria, (2) logic in the coded application, and (3) needs and uses of edit checks to detect incomplete data elements put into the application.

-Similar independent teams should review the operation of these applications shortly after they are implemented. The objectives would be to evaluate the adequacy of the decisionmaking criteria in an operational environment and to provide for early detection of any bad decisions. This would allow for early correction of problems.

-Some form of cyclical system monitoring of actions initiated by operational automated decisionmaking applications should exist. Teams composed of (but not restricted to) designers, users, and auditors could analyse application-initiated actions to (1) see if desired results were achieved in the best way, (2) identify unforeseen circumstances that would require modifying the application, (3) determine that the actions were as the user and designer intended, and (4) insure that decisionmaking was not adversely affected by incomplete data not being screened by an edit check.

-The designer and user should be physically located in the same place during design phases to allow for constant communication. In effect, the design would be a joint effort and would help to insure that adequate decisionmaking criteria were contained in the application.

-Priorities should be established for software modification (changes) which are at least partially based on the cost of continuing incorrect automatic actions if no changes are made within a short time.

-The initiator of the needed software modification (for example, headquarters, user, audit team and/or others) should be informed about the status of the change and be provided with confirmation that the changes have been made." [22]

E. COST IMPLICATIONS

"The cost of increased overhead created by additional checking verification should not be greater than the value

of the resources being protected or the use of a secure system will be deterred." [24]

The aspects of determining the cost of privacy include tangible and intangible factors. Past research has not accumulated a significant amount of statistical information on the subject and therefore concrete totals in time, manhours expended and money are not readily available to the general public. The tangible cost factors include the number of data subjects who will make inquires, the amount of executive personnel time necessary to handle data disputes, programming time to develop software to handle Privacy Act requirements and personnel training. There are three major facets of cost. Legitimate costs include conversion and operating costs. The third is improper costs or those items or procedures which have been planned previously, but are now mandatory and are charged to privacy legislation. Examples include installing more physical security hardware, purging or destroying obsolete data, installing a new data management system, or no longer collecting more personal information than is required. It is also conceivable that organizations may charge the privacy budget with miscellaneous expenses such as changing programs or re-converting application systems.

The National Bureau of Standards has published "A Computer Model to Determine Low Cost Techniques to Comply with the Privacy Act of 1974" which was developed by Goldstein and Seward. [25, 42] The legitimate costs of privacy are portrayed in this model. This report, however, warns of using the figures in specific cases since the factors influence each agency in specific degrees. The elements used in the model are applicable to many agencies. however, it is left to the discretion of each individual installation to determine to what degree each factor affects their total cost and which elements may or may not be

applicable or are not included in the model. The twenty compliance steps (techniques) analysed by the model fall into four general categories :

1. Subject Access Requirements
2. Subject Control Requirements
3. Data Usage Requirements
4. Operating Procedure Requirements

To provide clarity, the variable names used as input to the model are in parenthesis after each compliance step.

1. Subject Access Requirements

A. Notify each subject of the existence and content of his record.

(Record existence notification)

B. Respond to inquiries from data subjects concerning the existence and content of their records.

(Record existence inquiry)

C. Respond to inquiries from data subjects concerning the uses of their records.

(Record uses inquiry)

D. Respond to complaints from data subjects concerning the accuracy of their records.

(Data accuracy inquiry)

2. Subject Control Requirements

A. Notify each subject whether he is obligated to provide data.

(Data supply obligation notification)

B. Obtain the consent of the data subject for each use of the data.

(Consent for additional use)

C. Obtain the consent of the data subject before transferring data to a less protected system.

(Consent to transfer data)

3. Data Usage Requirements

A. Check the authorization of each request for data.

(Check usage authorization)

B. Maintain a log of all accesses to personal data.

(Usage log maintenance)

C. Include the data subject's statement with any release of disputed data.

(Subject claim dissemination)

D. Send the subject's statement to all past recipients of disputed data.

(Retroactive claim dissemination)

E. Assure that any system to which data is transmitted will provide adequate protection.

(Record transmission)

F. Notify the subject before data is released in compliance with legal process.

(Legal process notification)

4. Operating Procedure Requirements

A. Assure the accuracy and completeness of all records.

(Data accuracy)

B. Include any additional data needed to give a fair picture.

(Additional data)

C. Store a subject's statement of dispute with his record.

(Subject claim storage)

D. Protect against threats and hazards to the security of the data.

(Physical security)

E. Train all users in appropriate privacy procedures.

(User training)

F. Assure that his system meets all of the requirements.

(System assurance)

G. Publish a description of his system where it will be seen by most data subjects.

(Public notice)

The model then requires a determination of the value of various attributes which describe a personal data system. In all, seventy-five pieces of data are required. Examples are the size of the data base, volume of transactions, and the number and types of users. These factors are also used to determine whether a system has on-line capability and if a data management package is used. Certain attributes are matched with the regulatory requirements in a matrix format. These are then analysed to produce two output formats (reports). "The first level of output from the model consists of estimates of the incremental amounts of various resources needed to meet each requirement. Incremental resource demands are calculated in order to provide an indication of what new costs would be incurred specifically because of the privacy legislation, and to avoid the probably insolvable problem of deciding what share of certain costs should be attributable to privacy, and what to other objectives. The impact model also distinguishes between conversion costs which are incurred only once to bring a system into compliance with the regulations, and ongoing costs which must be added to 'preprivacy' operating costs." [25]

Conversion (nonrecurring) cost factors include physical security, operator and user training in privacy-oriented procedures, and programming required to develop legislatively mandatory capabilities. This is the first output format which includes cost totals for each requirement.

Types of ongoing costs encompass maintaining an accurate data base and handling complaints and inquiries from data subjects. (The second section of the output consists of these expenses.) It is suggested the reports be placed side-by-side for most efficient analysis. "The general resource categories which are considered are: manpower, data storage, information processing, data communications, and capital (which includes various items of equipment and supplies). Each of these categories is broken down into several subdivisions." [25]

The model uses the following headers respectively: administration, storage, processing, data transmission, and capital. Additionally, the number of programming man-hours is listed.

"Once the resource demands of each requirement have been computed, they are converted to money amounts using factors appropriate for the specific installation, and are then aggregrated by resource and by requirement. This enables the quick identification of high-cost requirements and of resource areas experiencing heavy demands." [25]

It is obvious that not all data bank systems will encounter the same level of conversion and ongoing costs. The data banks with information already publically available or of low sensitivety need to implement features that guarantee data integrity and prevent user interference with each other. More sensitive information in on-line, shared and integrated data bank systems, however, may require the installation of all known protection features.

Certain conclusions reached by Goldstein about relative costs are worth noting. With reguard to conversion costs, three areas were expensive. The first is the cost of new forms which should include a notification of the rights of

the data subject when providing information on the form; second, the cost of installing a "satisfactory" physical security system; and third, employee training in the use of new procedures. In some instances programming significantly increases the cost of conforming to legislation. (Goldstein suggests using general data base management packages to decrease conversion costs).

Under the category of operating costs, the most expensive areas were: searching a file for the records of those individuals who inquire about the data in the record and which organizations have the record and the executive personnel time required to process data subject's complaints about the accuracy of their records. The findings of the study by Goldstein are still preliminary and in some instances his conclusions are not surprising. Until this model is used with other types of computer installations, it is still nebulous as to what the costs of privacy legislation are.

III. CONCLUSIONS

The privacy issue is extremely complex in nature. The proper balance of protecting individual rights through management procedures, data considerations, and security measures is needed to insure compliance with legislation. This reevaluation of current systems and technology is intended to bring out important factors in maintaining compliance with legislation. To achieve the proper balance between the right of the individual and the rights of industry and government with regard to personal information is the ultimate ideal goal.

Insuring individual privacy protection extends from the state level to beyond a country's physical geographical border. [11,52] The nine Common Market countries have recognized the need for standard legislation on the international scale as is evidenced by the survey currently being conducted by the Commission of the European Communities. [11] One important fact is that the data processed in each country is not legally protected once it is outside its borders. The issue is yet to be resolved in the United States of America and Canada. It could have an enormous impact on private industry if H.R. 1984 becomes a law.

The questions concerning management of personal information still to be resolved are most importantly (1) if the computer installation personnel have implemented all possible measures through administrative, training and security procedures to protect an individual's personal data and the personal data is still obtained by unauthorized

means, who is responsible and liable for legal penalties? (2) if the 'state of the art' technology is yet to solve the problem of a completely secure automated system, is the computer industry legally responsible for personal data obtained thrcugh currently unsolvable technological methods? and (3) to what extent should the computer manager implement procedures to insure that privacy legislation is complied with?

Data accuracy can best be achieved through input validation procedures. If however, that data is inaccurate due to improper entry by the individual who is the subject of that data, then who is legally responsible? Again, a relationship of trust must be reinforced between the data subject and the computer industry. Legally, the industry is not covered and unless they establish some protection procedures, a lawsuit could result.

The problems associated with hardware lie mainly with the telecommunication systems (electronic emanations) and older computer systems which do not have all the internal security checks and protection mechanisms that are in the third-generation systems. With regard to electronic emanations, it is the researchers who must solve this problem. As for older computer systems, if computer installations have to change equipment to comply with legislation, it would be costly.

One major problem is the compatability of "legal records" with "computer records". Legally, the term record could mean only a part of a computer record. This means reorganizing files and a new method of structuring data must be achieved. The complication of having a variety of data sensitivity levels in a computer record can be costly to the computer installation. the issue is even more complex with

the requirement to retrieve all data held on a data subject should the individual request it.

The data structure problem is both hardware and software connected. Limitations exist in the physical storage capacity of the equipment and the programs utilized in the processing of the data must be reevaluated for possible modification to a new system. Software auditing procedures must be implemented to insure unauthorized access is not possible, as well as unintentional modification of data.

The cost of implementing privacy legislation has been analysed by Goldstein and Seward. Although it has only been used on a few types of systems (internal, financial, and governmental) the results are promising. The Purdue Information Privacy Research Center is currently conducting research on the economic impact of privacy. [17] The results of this study should be of great value to the computer industry.

This discussion has mentioned various procedures, technological and administrative, to be implemented in regard to decreasing unauthorized access and increasing data accuracy as is required by the privacy legislation in effect today. It is not intended to cover all areas of the privacy situation nor answer all questions. It is intended to emphasize major considerations faced by the computer industry with the advent of privacy legislation.

BIBLIOGRAPHY

1. Adcock, William O. and Moore, Anne M., "Consumers Unenthusiastic About EFT/Privacy Rules", Computerworld, September 13,1976, p.25.

2. "Alan Westin's Keynote Address", Communications of the ACM, Volume 18, Number 12, December 1975, p. 747.

3. Anderson,James P., Computer Security Technology Planning Study,U.S.A.F. Electronics Systems Division, Tech Report 73-51, Vol II,October 1972.

4. "Approaches to Controlling Personal Access to Computer Terminals", Proceedings of the 1975 Symposium Computer Networks: Trends and Applications, IEEE Computer Society 1975, Cotton, Ira W. and Meissner, Paul, p.32-39.

5. Arnst, Catherine, "Privacy Protection Seen Backfiring on Individuals",Computerworld, May 10,1976, p.6.

6. Avison, D.E. and Crowe, T., "Computers and Privacy", Computer Bulletin, Series 2, Number 7, March 1976.

7. Ball, Leslie D. and Wood , Steven D., "Computer Security in Concentrated Information Systems", Arizona Business, March 1976.

8. "Bank, Phone, Credit Records Target of Koch Privacy Bill", Computerworld, February 21,1977, p.8.

9. Becker, Louise E. G., "Privacy: Information Technology Implications," Issue Brief Number IB4105, The Library of Congress, Congressional Research Service, January 20, 1976.

10. Bushkin,A.A. and Schaen,S.I., The Privacy Act of 1974: A Reference Manual for Compliance,System Development Corporation, 1976.

11. "Common Market Seeking Common Privacy Policy", Computerworld, February 21,1977, p.11.

12. French, Nancy, "Abuse by Authorized Called Privacy Law Concern", Computerworld, April 26,1976, p.14.

13. French, Nancy, "...But Credit Reporters See More Laws Harmful", Computerworld, August 9,1976, p.3.

14. French, Nancy, "Federal Agencies Need Procedures for Privacy Act", Computerworld, December 25,1975, p.5.

15. French, Nancy, "High Court Vote Spurs Action on Tunney Privacy Bill",Computerworld, March 29,1976, p.4.

16. French, Nancy, "Limiting Access to Tax Return Could Hamper Federal Work, Privacy Group Told in Hearings",Computerworld, March 29,1976, p.7.

17. French, Nancy, "Privacy Act Hit as Administered But Not Enforced", Computerworld, November 15,1976, p.9.

18. French, Nancy, "Privacy Protection in '76: A Hot Topic on Every Level", Computerworld, December 27,1976/January 3,1977, p.8.

19. French, Nancy, "Problems Cited in Discontinuing SSN as Identifier", Computerworld, August 9,1976, p.6.

20. French, Nancy, "Proxmire Decries FCRA Limitations", Computerworld, August 9,1976, p.2.

21. French, Nancy, "security Measures Not Means to Privacy Ends: OTP", Computerworld, January 31,1977, p.9.

22. GAO Report, "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government", April 23, 1976.

23. GAO Report, "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities", May 10,1976.

24. Gerberick, D.A., and others, Privacy, Security and the Information Processing Industry , Association for Computing Machinery, 1976.

25. Goldstein, Robert C., "The Costs of Privacy", Datamation, Vol 21, No. 10, p. 65-69, October 1975.

26. Goldstein, Robert C., The Cost of Privacy, (Honeywell Information Systems, Inc., 1975)

27. Government and Privacy, American Enterprise Institute, Washington, D. C., 1971.

28. "Government Drive Hits Possible Privacy Abuses by Its Computers", Commerce Today, p.9, Dec 9,1974.

29. Great Britain. Parliament. Cmnd.6353, December 1975, "Computers and Privacy".

30. Great Britain. Parliament. Cmnd.6354, "December 1975, "Computers: Safeguards for Privacy".

31. Hanlon, Joe, "UK Job-Matching Plan Attacked on Privacy Grounds",Computerworld, May 10,1976, p.9.

32. Hanus, Jerome J., "Privacy: Concepts and Problems," Issue Brief Number IB74123, The Library of Congress, Congressional Research Service, January 12, 1976.

33. Herbert, John P., "Proposed IRS System May Pose Threat to Privacy, Study Warns", Computerworld, February 21,1977, p.1.

34. Hoffman, L.J., "Computers and Privacy: A Survey", Computing Surveys, Vol. I, No. 2, p. 85 - 103, June 1969.

35. Holmes, Edith, "Study Questions Applicability of Privacy Act to NDR", Computerworld, January 10,1977, p.12.

36. "How The Privacy Act Impacts on DOD," Commander's Digest , Volume 18, Number 7, August 14, 1975.

37. "Integrity and Security of Personal Data",EDP Analyzer, Volume 14, No 4, April 1976.

38. Martin J., Security, Accuracy and Privacy in Computer Systems , Prentice - Hall, Inc., 1973.

39. Miller, Arthur R., The Assault on Privacy (Ann Arbor, Michigan: The University of Michigan Press, 1971).

40. Muftic, Sead, "Social Aspects of Computer Networks", Management Datamatics, Vol. 4 (1975), No. 6, p. 207 -211.

41. National Bureau Of Standards Special Publication 404, Approaches to Privacy and Security in Computer Systems, C. R. Renninger, ed., September 1974.

42. National Bureau of Standards NBSIR 76-985, A Computer Model to Determine Low Cost Techniques to Comply with the Privacy Act of 1974, Dr. R. C. Goldstein and Dr. Henry H. Seward, February 1976.

43. National Bureau of Standards and Association for Computing Machinery LC 1062, Executive Guide to Computer Security , D.K.Branstad and S.K.Reed, June 1974.

44. National Bureau of Standards NBS Technical Note 876, Exploring Privacy and Data Security Costs - A Summary of a Workshop , J. L. Berg, ed,. August 1975.

45. National Bureau of Standards FIPS Pub 31, Guidelines for Automatic Data Processing Physical Security and Risk Management ,R.V. Jacobson, June 1974.

46. National Bureau of Standards FIPS Pub 41, Computer Security Guidelines for Implementing the Privacy Act of 1974 , May 30, 1975.

47. "NETWORK VIABILITY: Economic, Legal, and Social Considerations", The Annual IEEE Computer Society International Conference (COMPCON 73), Enslow Jr., Phillip H., p. 7-9.

48. Niblett, G.B.F., Digital Information and the Privacy Problem , Organization for Economic Co-operation and Development Publications Center, p.21-25, 1971.

49. Office of Management and Budget Circular No A-108, Subject: Responsibilities for the maintenance of records about individuals by Federal Agencies , 1 July 1975. Subject: Guidelines for Implementing Section 3 of the Privacy Act of 1974 .

50. Parker, Donn B., "Rules of Ethics in Information Processing", Communications of the ACM, Vol. 11, No. 3, March 1968, p. 198 - 201.

51. "Privacy update...An interview with Congressman Barry M. Goldwater Jr.", Data Management , February 1976, p.30-32.

52. "States Busy With Privacy Laws", Computerworld, September 13,1976.

53. The Freedom of Information Act (5 U.S.C. 552, as amended by P.L. 93-502)

54. The Privacy Act of 1974 (5 U.S.C. 552a, created by P.L. 93-579)

55. U.S. Department of Health, Education and Welfare, DHEW Publication No. (OS) 73-97, "Records, Computers and the Roghts of Citizens", Report of the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973.

56. United States Senate, Federal Data Banks and Constitutional Rights, Volumes 1, 3, 4, and 5, U. S. Government Printing Office, Washington, D. C., 1976.

57. United States Senate, Privacy - The Collection, Use, and Computerization of Personal Data, Parts 1 and 2, U.S. Government Printing Office, Washington, D. C., 1974.

58. "VA Says Target System Meets Privacy Act Demands", Computerworld, September 13,1976, p.7.

59. Weston, Alan F., and Baker, Michael A., Databanks in a Free Society (New York, New York: The New York Times Book Company, 1972).

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93940	2
3.	Department Chairman, Code 52 Department of Computer Science Naval Postgraduate School Monterey, California 93940	1
4.	Professor N. F. Schneidewind Department of Operations Research Naval Postgraduate School Monterey, California 93940	1
5.	LT L. V. Rich, USN USS Dubuque FPO San Francisco, California 96601	1
6.	LT Carol Jean Janssens, USN, Code 0302 Naval Postgraduate School Monterey, California 93940	1

Thesis
J2913
c.1

170378

Janssens
Privacy legislation and its implication toward the computer industry.